Personal data and technology

Esther Cerdeño Argüelles
IT Graduate. Universidad Politécnica de Madrid
IT Assistant Manager
MAPFRE RE (Madrid- Spain)

The information contained in the computer files of companies, public organisations, educational and health establishments among others, represents a stock of enormous value, because it accounts for a very significant portion of the knowledge accumulated during the course of their activities. As far as individuals are concerned, the widespread use of IT instruments means that companies have increasingly more complex, sophisticated and pertinent data. Although paper files containing personal information have always existed, IT means that they can now be collected in databases that can be processed automatically with much greater possibilities for analysis and use. The corporate world is making a significant effort to adapt its structures and procedures to the requirements of specific laws. A sector that is significantly affected is insurance and reinsurance companies.

Basic aspects of the Spanish LOPD (Ley Orgánica de Protección de Datos - Data Protection Act)

General provisions

- Applies to personal data recorded on any **physical medium capable** of being processed.
- Protects the *personal and* **familial privacy** of individuals, owners of the data, interested or affected parties.
- Defines what personal data and specially protected data is; files, managers and processing, affected party, data transfer.
- Establishes the quality of data : adequate, relevant and not excessive.
- Provides the affected parties with the right to see and approve their data if it is not collected directly from the affected party, who has to be expressly informed, unless the law provides otherwise.
- Provides the right to challenge assessments, access to data, correction and deletion.

Sector provisions

- Creation, notification, registration, processing of publicly and privately owned files.

International movement of data

- Prohibited to those countries that do not have a comparable level of protection to that provided by the LOPD. In principle, the authorisation of the director of the Data Protection Agency is required.

Data Protection Agency

- A public entity with its own legal status and full public and private capacity, which acts independently of the Public Authorities in accordance with Law 30/l992 of 26th November.

Infringements and Sanctions

- Infringements classified according to treatment of data, sanctions and periods of prescription:

Minor:	EUR 601.01	to	EUR 60,101.21	period of prescription 1 year
Serious:	EUR 60,101.21	to	EUR 300,506.05	period of prescription 2 years
Very serious:	EUR 300,506.05	to	EUR 601,012.10	period of prescription 3 years

Legislation

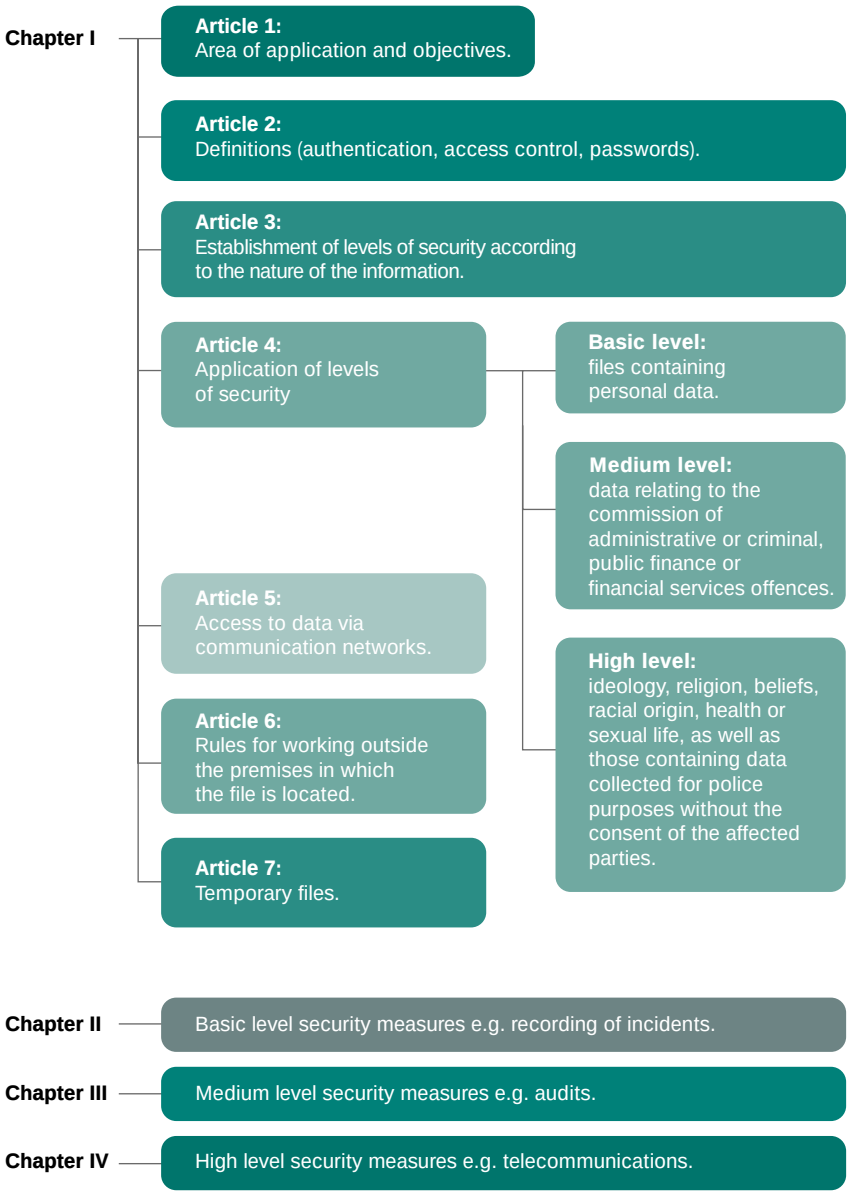
The improper use of personal databases could harm or prejudice the interested parties. Therefore, States have developed extensive regulations.
In Spain these are ruled by the Organic Law on Data Protection (LOPD). Similar sets of laws have also been adopted in other European countries.

- SPAIN: Organic Law 15/1999, of 13th December on the protection of data of a personal nature.

In 1978, the Spanish Constitution restricted the use of IT to protect the privacy of its citizens in Article 18.4, laid down when technological advances and cheaper systems made it necessary to promulgate the legislation in order to guarantee and protect data of a personal nature.

In 1992, Organic Law 5/1992 of 29th October on the regulation of the automatic processing of data of personal nature (LORTAD) was passed. This law has been replaced by Organic Law 15/1999 of 13th December on the protection of data of a personal nature (LOPD).

SPAIN: Royal Decree 994/1999 Regulation of Security Measures for Computerised Files containing Personal Data



A measure which is recommendable in any corporate environment is to establish a close relationship between the *technology, legal, physical security and human resources departments,* in order to define existing data levels and possible safety measures to be implemented.

The cost of a technical set-up which protects the privacy of personal data must not be made subordinate to a possible financial sanction, or even worse, the loss of corporate image.

Royal Decree 994/1999 which approves the Regulation of Security Measures for computerised files that contain personal data was established to support the Spanish LOPD.

The regulations are split into four chapters which establish the technical and organisational measures necessary to guarantee the security that computerised files, processing centres, locations, equipment, systems, programmes and the people who work on the computerised processing of personal data must provide.

The said regulations specify the production of a *Security Document* with specifications for each level, with all the measures to guarantee the confidentiality of the personal data as well as any impact on its processing. These measures may be of a technical or organisational nature, relating to the nature of the data and the need to guarantee its integrity and confidentiality.

EUROPEAN UNION: Directive 2002/58/EC of the European Parliament and Council

There are several rules relating to the protection of personal data within the European Union. Directive 2002/58/EC of the European Parliament and Council on the processing of personal data and protection of privacy in electronic communications was approved on 12th July 2002. On 19th November 2003, the European Parliament reached agreement on the proposed creation of ENISA (European Network and Information Security Agency) designed to co-ordinate information security among Member States.

Adjustment of the LOPD to a corporate environment

Technological progress has produced tools to facilitate compliance with the LOPD. A

Fundamental Aspects of a Security Document

- **Area** of application of the document including specification of the protected resources.
- **Rules** and measures designed to guarantee the level of security required in the regulations.
- **Personnel** duties and obligations.
- **Structure** of files containing personal data and description of the information systems which process them.
- **Procedure** for notification, handling and responding to incidents.
- **Procedure** for making back-ups and data recovery.

confidentiality assessment of the data contained in the files (low, medium or high level) will determine the type of measures to be implemented. We give below a diagram that illustrates a series of technical measures in harmony with the Spanish LOPD, which can be implemented within a corporate environment, not forgetting that in this environment the resources of the systems are shared but where in turn, *proper access* to data of a personal nature must be *guaranteed*.

Insurance and reinsurance companies

Insurance companies hold and process important personal data which can refer to health, accidents and property among other things. Therefore, in Spain there is a rising concern in this sector with regard to appropriate compliance with the LOPD thus guaranteeing the protection of the personal data of their customers, employees and suppliers, also avoiding substantial sanctions.

As a specific measure of the LOPD and for medium and high level data throughout the corporate environment, there is an obligation to submit to an audit (internal or external) every two years. This is carried out with appropriate IT tools which, among other things, enable accesses to the systems to be consulted and situations representing incidents to be reproduced, revealing the condition of the data when it was modified.

"The cost of a technical set-up which protects the privacy of personal data must not be made subordinate to a possible financial sanction, or even worse, the loss of corporate image."

Within an insurance context, the following aspects are highlighted:

Principle of Purpose

The Principle of Purpose establishes that a company cannot use the data for a purpose other than that for which it was provided.

Transfer of data during the life of the policy

The personal data of an insured can only be transferred with the consent of the interested party, especially in the case of information relating to his health and generally speaking any data that ranks as "specially protected".

The transfer of the said data to reinsurance companies can be covered by the intrinsic need for basic information for a reinsurance policy on the person or persons who are the subject of cover, so that it can be appropriately designed and quoted by the reinsurer.

Conclusions

It is important to establish an adequate flow of information on current legislation about processing data of a personal nature within companies. Various alternatives are appearing in all areas in order to guarantee the security of personal data and the right to privacy. In the case of Spain, this work has been carried out within the framework of the European Union, illustrated within a corporate environment and revealing several points of application to the insurance and reinsurance sector.

The corporate world has to understand that lack of knowledge of the law or the cost of introducing a security policy on personal data, does not justify non-compliance.

Useful addresses

- www.rediris.es/cert/links/legal.es.html
- www.upco.es
- www.microsoft.com/spain/seguridad
- www.agpd.es
- www.delitosinformaticos.com
- www. portaley.com/protecciondatos/

Diagram of technological measures in a corporate environment

Information on procedures for complying with the law	**Creation** of a Portal in the Intranet which enables information to be distributed on the law and how to apply it. **Advice** on setting up the equipment to enable users to be aware of the security rules.
Identification and Authentication	**Identifying** the user to the system by means of a user password. **Use** of Directory Services (LDAP standards: *Lightweight Directory Access Protocol*): single entry point for user administration, file location, printer for authenticated users. **Definition** of user groups and/or profiles for access to applications.
	Establishing policies of secure passwords: **Minimum length:** 6 characters **User-month** or month-user type of passwords not acceptable. **Compulsory** expiry every 45 days with 5 day margin to change the code. **Use** of the same code not permitted until "n" exchanges have occurred. **User** accounts blocked if the password is incorrectly keyed in on 5 consecutive attempts.
Logical access control	**Use** of file records *(logs)* of correct, failed or non-permitted access events generated by the network systems. **Use** of database procedures or functions for storing records accessed in tables. **Use** of tools for user access identification and ability to reproduce status of the data at any time.
Back-up and recovery	**Automation** and computerisation of creating copies and file recovery. **Inventory** and labelling of media (sets of tapes). **Keeping** a record of access to the data contained in the file recovery devices. **Data recovery** application forms. **Storage** in special cupboards protected by locks and passwords, and kept in a different room from the computers or even in different buildings. **Encryption** of high level data when the media leaves the building. **Record** of devices coming in and going out.
File declaration	**By means** of a programme available from the Data Protection Agency for generating documents associated with files that specify the responsible party, access, name, security, purpose and structure. **File declaration** by data transmission. **Reception** of record confirmation by post.
Auditing : High and medium level	**Compulsory** internal or external auditing of data processing using a tool which enables you to consult accesses, reproduce situations, etc. **Verification** of current instructions and procedures.
Physical access control	**Computer rooms** with access restricted to registered personnel, directors and security personnel. **Key** or card access system. **Record** of correct and incorrect accesses. **Cameras** at access doors.
Telecommunications: High level	**Encryption** of data if travelling over non-local networks. **Use** of VPN (Virtual Private Network) **Use** of IPS (Internet Protocol Security) protocols **Integrity** and encryption technologies.